ON LINEAR DIOPHANTINE EQUATIONS AND FIBONACCI NUMBERS

Michael Drmota

Technical University of Vienna

Abstract. By Minkowski's theorem on linear forms it is shown that the homogeneous linear diophantine equation $a \cdot x = a_1x_1 + \cdots + a_Kx_K = 0$ ($K \geq 2$, $a_i \neq 0$, $1 \leq i \leq K$) has a non-zero integral solution x with $r(x) \leq (K-1) \cdot r(a)^{1/(K-1)}$ (where $r(y) = \prod_{i=1}^{K} \max(|y_i|, 1)$). It turns out that it very difficult to decide if the exponent $1/(K-1)$ is optimal or not. (Of course the case $K = 2$ is trivial.) It is shown that there exist integral coefficients $a \in \mathbf{Z}^K$ with arbitrarily large $r(a)$ such that every non-zero integral solution of $a \cdot x = 0$ satisfies $r(x) \geq c_K r(a)^{1/K}(\log r(a))^{-K}$. In the non-trivial case $K = 3$ coefficients like $a = (F_{6m+1}, F_{6m+2}, F_{6m+2} + 1)$, where F_n denote the usual Fibonacci numbers, can be used to prove the optimality of the exponent $1/(K-1)$.

Furthermore the connection between this diophantine problem and the discrepancy of linear functions $f(t) = at \mod 1$ is discussed.

1. Introduction

Let us consider a homogeneous linear diophantine equation

$$a \cdot x = a_1x_1 + \cdots + a_Kx_K = 0 \tag{1.1}$$

with integral coefficients $a = (a_1, \ldots, a_K) \in (\mathbf{Z} \setminus \{0\})^K$ ($K \geq 2$). A simplified version of Siegel's lemma [Sie] ensures that there are non-zero integral solutions $x = (x_1, \ldots, x_K) \in \mathbf{Z}^K$ of (1.1) with

$$||x|| \leq (K-1) \cdot ||a||^{\frac{1}{K-1}}, \tag{1.2}$$

where $||(y_1, \ldots, y_K)|| = \max_{1 \leq i \leq K} |y_i|$. It is well known that the exponent $1/(K-1)$ in (1.2) is best possible (cf. [Sch]).

In this paper we will show that there are also non-zero integral solutions $x \in \mathbf{Z}^k$ of (1.1) with

$$r(x) \leq (K-1) \cdot r(a)^{\frac{1}{K-1}}, \tag{1.3}$$

where

$$r((y_1, \ldots, y_K)) = \prod_{i=1}^{K} \max(|y_i|, 1). \tag{1.4}$$

Notice that (1.3) neither implies (1.2) nor is implied by it.

It seems to be a difficult problem to decide in general whether the exponent $1/(K-1)$ in (1.3) is optimal or not. Of course, for $K = 2$ the answer to this question is trivially affirmative. It is interesting that coefficients like $a = (F_{6m+1}, F_{6m+2}, F_{6m+2}+$

1), where F_n are the usual Fibonacci numbers, can be used to show that the exponent $1/(K-1)$ is optimal for $K=3$, too. In general the author only knows that there are coefficients $a \in (\mathbf{Z}\setminus\{0\})^K$ $(K \ge 2)$ with arbitrarily large $r(a)$ such that all non-zero integral solutions x of (1.1) satisfy

$$r(x) \gg r(a)^{\frac{1}{K}} (\log r(a))^{-K}. \tag{1.5}$$

This will be proved in a non-constructive way.

It should be mentioned that the problem to get some information about the smallest $r(x)$ of non-zero solutions x of (1.1) is related to the discrepancy of linear functions $f(t) = at \mod 1$, $t \in [0,1]$ (see [Dr]). Let $g : [0,1] \to \mathbf{R}^K/\mathbf{Z}^K$ be a measurable function. Then the discrepancy $D(g(t))$ is defined by

$$D(g(t)) = \sup_{I \subseteq \mathbf{R}^K/\mathbf{Z}^K} \left| \int_0^1 \mathbf{1}_I(g(t))\, dt - \lambda_K(I) \right|, \tag{1.6}$$

where $I \subseteq \mathbf{R}^K/\mathbf{Z}^K$ is a rectangle $I = [a_1, b_1] \times \cdots \times [a_K, b_K] \mod 1$ with $0 < b_i - a_i < 1$ $(1 \le i \le K)$, $\mathbf{1}_I$ is the characteristic function of I, and λ_K the K-dimensional Lebesgue measure. By Koksma-Hlawka's and Koksma-Erdös-Turan's inequality [KN] for functions we have for $f(t) = at \mod 1$, $a \in \mathbf{Z}^K$,

$$\max_{a\cdot x=0, x\ne 0} \frac{1}{r(x)} \ll D(at) \ll \sum_{a\cdot x=0, x\ne 0} \frac{1}{r(x)}. \tag{1.7}$$

Questions related to the discrepancy of linear functions will be discussed in a final section.

2. An Alternative to Siegel's Lemma

Theorem 1. *Let $K \ge 2$ and $a = (a_1, \dots, a_K) \in (\mathbf{Z}\setminus\{0\})^K$ any integral lattice point. Then there exists a non-zero integral solution $x = (x_1, \dots, x_K) \in \mathbf{Z}^K$ of the homogeneous linear diophantine equation*

$$a \cdot x = a_1 x_1 + \cdots + a_K x_K = 0 \tag{2.1}$$

with

$$r(x) \le (K-1) \cdot r(a)^{\frac{1}{K-1}}. \tag{2.2}$$

Proof. Define linear forms $L_i(x)$ $(1 \le i \le K)$ by

$$\begin{aligned} L_i(x) &= x_i \quad \text{for} \quad 1 \le i \le K-1 \\ L_K(x) &= a \cdot x \end{aligned} \tag{2.3}$$

with determinant $\Delta = a_K \ne 0$. Then by Minkowski's theorem for linear forms there is a non-zero intergral point x with

$$\begin{aligned} |L_i(x)| &\le \frac{r(a)^{\frac{1}{K-1}}}{|a_i|} \quad \text{for} \quad 1 \le i \le K-1 \\ |L_K(x)| &< 1, \end{aligned} \tag{2.4}$$

because
$$\prod_{i=1}^{K-1} \frac{r(a)^{\frac{1}{K-1}}}{|a_i|} = |a_K| = |\Delta|. \tag{2.5}$$
But $L_K(x)$ is an integer. So x solves the linear diophantine equation $a \cdot x = 0$ and we can estimate x_K by
$$|x_K| \leq \frac{1}{|a_K|} \sum_{i=1}^{K-1} |a_i x_i| \leq (K-1) \cdot \frac{r(a)^{\frac{1}{K-1}}}{|a_K|}. \tag{2.6}$$
Assume for a moment that $r(a)^{\frac{1}{K-1}}/|a_i| \geq 1$ for $1 \leq i \leq K-1$ and that $(K-1) \cdot r(a)^{\frac{1}{K-1}}/|a_K| \geq 1$. Then
$$r(x) \leq (K-1) \cdot \prod_{i=1}^{K} \frac{r(a)^{\frac{1}{K-1}}}{|a_i|} = (K-1) \cdot r(a)^{\frac{1}{K-1}}, \tag{2.7}$$
as proposed. For $K = 2$ this assumption is always satisfied. So let $K > 2$ and assume that (2.2) is true for all dimensions $< K$ and let I be the set of those i with $r(a)^{\frac{1}{K-1}}/|a_i| < 1$. Without loss of generality we can assume that $K \notin I$. Furthermore we always have $K - |I| \geq 2$. So we can conclude by induction that there is a non-zero integral solution x with $x_i = 0$ for $i \in I$ and
$$r(x) \leq (K - |I| - 1) \left(\prod_{j \notin I} a_j \right)^{\frac{1}{K-|I|-1}}. \tag{2.8}$$
But $|a_i| > r(a)^{\frac{1}{K-1}}$ for $i \in I$ implies that $r(x)$ can be estimated by
$$r(x) \leq (K-1) \left(\prod_{i=1}^{K} a_i \right)^{\frac{1}{K-|I|-1}} r(a)^{-\frac{|I|}{(K-1)(K-|I|-1)}} = (K-1) \cdot r(a)^{\frac{1}{K-1}}. \tag{2.9}$$
So we are done. □

3. Lower Bounds and Fibonacci Numbers

For $K = 2$ the exponent $1/(K-1)$ of Theorem 1 is trivially optimal. You only have to choose coprime $a_1, a_2 \in \mathbf{Z} \setminus \{0\}$. Then every non-zero integral solution of $a_1 x_1 + a_2 x_2 = 0$ is given by $x_1 = m a_2$, $x_2 = -m a_1$ with $m \in \mathbf{Z} \setminus \{0\}$. So $r(x) = m^2 r(a) \geq (2-1) \cdot r(a)^{\frac{1}{2-1}}$.

As indicated in the introduction it seems to be very difficult to settle this optimality question in general. With help of Fibonacci numbers we will prove that the exponent $1/(K-1)$ is optimal for $K = 3$.

Theorem 2. *Let $a = (F_n, F_{n+1}, F_{n+1} + (-1)^{n+1})$, where $n = \pm 1 \mod 6$ and F_n denote the usual Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. Then for every non-zero integral solution $x \in \mathbf{Z}^3$ of the homogeneous linear diophantine equation $a \cdot x = 0$, $r(x)$ is bounded below by*
$$r(x) \geq c_1 r(a)^{\frac{1}{2}}, \tag{3.1}$$

where c_1 is an explicitely computable positive real constant. Moreover, if $x_i \neq 0$, $x_j \neq 0$, ($i \neq j$, $i,j \in \{1,2,3\}$) are two components of any integral solution x of $a \cdot x = 0$ we have

$$|x_i x_j| \geq c_2 F_n, \tag{3.2}$$

where $c_2 > 0$ is explicitely computable, too.

In general the author can only prove the following simple theorem:

Theorem 3. *Let $K \geq 2$. Then there exist integral lattice points $a \in (\mathbf{Z} \setminus \{0\})^K$ with arbitrarily large $r(a)$ such that every non-zero integral solution x of the homogeneous linear diophantine equation $a \cdot x = 0$ satisfies*

$$r(x) \gg r(a)^{\frac{1}{K}} (\log r(a))^{-K}. \tag{3.3}$$

Proof. Let G be an arbitrary large positive integer. Consider some non-zero integral lattice point $x \in \mathbf{Z}^K$ with $||x|| \leq G$ and choose i_0 such that $x_{i_0} \neq 0$. Then the number of integral solutions $a = (a_1, \ldots, a_K)$ of $a \cdot x = 0$ with $G \leq a_i < 2G$ $(1 \leq i \leq K)$ is bounded by G^{K-1} because for any choice $a_i \in [G, 2G)$, $i \neq i_0$, there is at most one $a_{i_0} \in [G, 2G)$ with $a \cdot x = 0$. So

$$\begin{aligned} &\frac{1}{G^K} \sum_{a, a_i \in [G,2G)} \left(\sum_{0<||x||\leq G, a\cdot x=0} \frac{1}{r(x)} \right) \\ &= \frac{1}{G^K} \sum_{0<||x||\leq G} \frac{1}{r(x)} \left(\sum_{a, a_i \in [G,2G), a\cdot x=0} 1 \right) \\ &\leq \frac{1}{G} \sum_{0<||x||\leq G} \frac{1}{r(x)} \\ &\ll \frac{(\log G)^K}{G} \end{aligned} \tag{3.4}$$

implies that there is some $a \in \mathbf{Z}^K$ with $a_i \in [G, 2G)$ and

$$\sum_{0<||x||\leq G, a\cdot x=0} \frac{1}{r(x)} \ll \frac{(\log G)^K}{G}. \tag{3.5}$$

Therefore $G^K \leq r(a) < 2^K G^K$ and (3.5) ensure that for any non-zero integral x with $0 < ||x|| \leq G$ that solves $a \cdot x = 0$ we have

$$r(x) \gg G(\log G)^{-K} \gg r(a)^{\frac{1}{K}} (\log r(a))^{-K}. \tag{3.6}$$

For $||x|| > G$ (3.6) is trivial. So Theorem 3 is proved. □

For the proof of Theorem 2 we will use two elementary lemmata:

Lemma 1. *Let* p, q *be positive coprime integers and*

$$\frac{p}{q} = [a_0; a_1, a_2, \dots, a_M] \qquad (a_M > 1) \tag{3.7}$$

the continued fraction expansion of p/q *and*

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n] \qquad (n \le M) \tag{3.8}$$

the principal convergents of p/q. *Then we have for* $n < M$

$$\frac{q}{2q_{n+1}} < |pq_n - qp_n| = \min_{q_n \le |x| < q_{n+1}, y \in \mathbf{Z}} |px + qy| < \frac{q}{q_{n+1}}. \tag{3.9}$$

Proof. (3.9) is a simple combination of Theorems 5 and 6 in Chapter I of [La]. □

Lemma 2. F_n *and* $F_{n+1} + (-1)^{n+1}$ *resp.* F_n *and* $F_{n-1} - 1$ *are coprime if and only if* $n \equiv \pm 1 \mod 6$. *In particlar we have*

$$\left.\begin{array}{r}(F_n, F_{n+1} + (-1)^{n+1}) \\ (F_n, F_{n-1} - 1)\end{array}\right\} = \begin{cases} 1 & \textit{for} \quad n \equiv \pm 1 \mod 6 \\ 2 & \textit{for} \quad n \equiv 3 \mod 6 \\ F_{\frac{n}{2}} & \textit{for} \quad n \equiv 0 \mod 4 \\ F_{\frac{n}{2}-1} + F_{\frac{n}{2}+1} & \textit{for} \quad n \equiv 2 \mod 4. \end{cases} \tag{3.10}$$

Furthermore the partial quotients a_i *of* $F_n/(F_{n+1} + (-1)^{n+1})$ *resp.* $(F_{n-1} - 1)/F_n$ *are equal to 1 for* $0 < i < n/2 - 2$.

Proof. By induction it follows that

$$(F_n, F_{n+1} + (-1)^{n+1}) = (F_{n-k} + (-1)^k F_k, F_{n-(k-1)} + (-1)^{k-1} F_{k-1}), \tag{3.11}$$

for

$$\begin{aligned} &(F_{n-k} + (-1)^k F_k, F_{n-(k-1)} + (-1)^{k-1} F_{k-1}) \\ &= (F_{n-k} + (-1)^k F_k, F_{n-(k-1)} + (-1)^{k-1} F_{k-1} - F_{n-k} - (-1)^k F_k) \\ &= (F_{n-k} + (-1)^k F_k, F_{n-(k+1)} + (-1)^{k+1} F_{k+1}). \end{aligned} \tag{3.12}$$

In particular for $k = 1$ we get $(F_n, F_{n+1} + (-1)^{n+1}) = (F_n, F_{n-1} - 1)$. Since $F_{n-(k-1)} + (-1)^{k-1} F_{k-1} > F_{n-k} + (-1)^k F_k$ for $k < n/2 - 2$ all partial quotients considered are equal to 1.

Now suppose that n is odd, say $n = 2k - 1$. Then $(F_n, F_{n-1} - 1) = (F_k + F_{k-1}, F_k - F_{k-1}) = (F_k + F_{k-1}, 2F_k)$. If $n \equiv 3 \mod 6$ then $k \equiv 2 \mod 3$ and so $F_k + F_{k-1}$ is even. Thus $(F_k + F_{k-1}, 2F_k) = 2(F_k + F_{k-1}, F_k) = 2$. If $n \equiv \pm 1 \mod 6$ then $F_k + F_{k-1}$ is odd and therefore $(F_n, F_{n-1} - 1) = 1$.

Finally suppose that n is even, say $n = 2k$. So $(F_n, F_{n-1} - 1) = (F_k + (-1)^k F_k, F_{k+1} + (-1)^{k-1} F_{k-1})$. Thus $(F_n, F_{n-1} - 1) = F_{k+1} + F_{k-1}$ for odd k. If k is even then $(F_n, F_{n-1} - 1) = (2F_k, F_k) = F_k$. So we are done. □

Remark. It should be noted that it is possible to calculate the continued fraction expansion of $F_n/(F_{n+1}+(-1)^{n+1})$ and $(F_{n-1}-1)/F_n$ of for $n \equiv \pm 1 \mod 6$ completely. We have

$$\frac{F_n}{F_{n+1}+(-1)^{n+1}} = \begin{cases} [0;\underbrace{1,\dots,1}_{6l-2},2,3,\underbrace{4,\dots,4}_{2l-2},3] & \text{for} \quad n = 12l-1 \\ [0;\underbrace{1,\dots,1}_{6l},5,\underbrace{4,\dots,4}_{2l-2},5] & \text{for} \quad n = 12l+1 \\ [0;\underbrace{1,\dots,1}_{6l+2},5,\underbrace{4,\dots,4}_{2l-1},3] & \text{for} \quad n = 12l+5 \\ [0;\underbrace{1,\dots,1}_{6l+2},2,3,\underbrace{4,\dots,4}_{2l-1},5] & \text{for} \quad n = 12l+7. \end{cases} \tag{3.13}$$

$$\frac{F_{n-1}-1}{F_n} = \begin{cases} [0;\underbrace{1,\dots,1}_{6l-2},5,\underbrace{4,\dots,4}_{2l-2},3] & \text{for} \quad n = 12l-1 \\ [0;\underbrace{1,\dots,1}_{6l-2},2,3,\underbrace{4,\dots,4}_{2l-2},5] & \text{for} \quad n = 12l+1 \\ [0;\underbrace{1,\dots,1}_{6l},2,3,\underbrace{4,\dots,4}_{2l-1},3] & \text{for} \quad n = 12l+5 \\ [0;\underbrace{1,\dots,1}_{6l+2},5,\underbrace{4,\dots,4}_{2l-1},5] & \text{for} \quad n = 12l+7 \end{cases} \tag{3.14}$$

You mainly have to use (3.12) and the relation $F_n - 4F_{n-3} = F_{n-6}$. It will be used in the proof of Theorem 2 that all partial quotients are bounded by 5.

Proof of Theorem 2. It sufficies to prove (3.2). For, if $x_1x_2x_3 \neq 0$ for some integral solution $x = (x_1, x_2, x_3)$ of $a \cdot x = 0$ then $r(x)^2 = |x_1x_2| \cdot |x_1x_3| \cdot |x_2x_3| \geq c_2^3 F_n^3$. Furthermore, if one component $x_i = 0$ then we have $r(x) \geq F_n^2$ because the coefficients F_n, F_{n+1}, $F_{n+1}+(-1)^{n+1}$ are coprime in pairs.

In order to prove (3.2) we will show that if x_i is a component of a solution x of $a \cdot x = 0$ with $0 < |x_i| < c_3 F_n^{1/2}$ for some positive constant c_3 then $|x_ix_j| \geq c_2 F_n$ for $j \neq i$.

We start with x_3. Since $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-1}$ implies $F_nF_n - F_{n+1}(F_{n-1} - 1) = F_{n+1} + (-1)^{n+1}$ and since F_n and F_{n+1} are coprime it follows that all integral solutions of $F_nx_1 + F_{n+1}x_2 + (F_{n+1} + (-1)^{n+1})x_3 = 0$ can be written as

$$\begin{aligned} x_1 &= -m_1F_n - m_2F_{n+1} \\ x_2 &= m_1(F_{n-1}-1) + m_2F_n \\ x_3 &= m_1 \end{aligned} \tag{3.15}$$

with $m_1, m_2 \in \mathbf{Z}$. The continued fraction expansion of F_n/F_{n+1} is given by

$$\frac{F_n}{F_{n+1}} = [0;\underbrace{1,\dots,1}_{n-2},2]. \tag{3.16}$$

So the principal convergents are exactly the quotients F_i/F_{i+1} $(i \leq n)$. Therefore Lemma 1 implies that

$$\min_{F_{i+1} \leq |m_1| < F_{i+2}, m_2 \in \mathbf{Z}} |-m_1F_n - m_2F_{n+1}| \geq \frac{F_{n+1}}{2F_{i+2}}. \tag{3.17}$$

Thus

$$|x_1x_3| \geq F_{n+1}\frac{F_{i+1}}{2F_{i+2}} \gg F_n \quad \text{for} \quad 0 < |x_3| < F_{n+1}. \tag{3.18}$$

By Lemma 2 the partial quotients of $(F_{n-1}-1)/F_n$ are equal to 1 for $0 < i < n/2-2$. So the principal convergents are again F_i/F_{i+1} for $0 < i < n/2-2$. Thus

$$|x_2x_3| \geq F_n\frac{F_{i+1}}{2F_{i+2}} \gg F_n \quad \text{for} \quad 0 < |x_3| < F_{[\frac{n}{2}-1]}. \tag{3.19}$$

But $F_{[\frac{n}{2}-1]} \gg F_n^{1/2}$. So we have shown that $|x_1x_3| \gg F_n$ and $|x_2x_3| \gg F_n$ for $0 < |x_3| \ll F_n^{1/2}$.

Next we will discuss solutions with small $|x_1|$. As above it can be shown that all integral solutions of $a \cdot x = 0$ can be written as

$$\begin{aligned} x_1 &= m_1 \\ x_2 &= -m_1(1+(-1)^{n-1}F_{n-1}) - m_2(F_{n+1}+(-1)^{n+1}) \\ x_3 &= -m_1F_{n-1}(-1)^n + m_2F_{n+1} \end{aligned} \tag{3.20}$$

with $m_1, m_2 \in \mathbf{Z}$. The continued fraction expansion of F_{n-1}/F_{n+1} reads as

$$\frac{F_{n-1}}{F_{n+1}} = [0;2,\underbrace{1,\ldots,1}_{n-4},2]. \tag{3.21}$$

So the quotients q_{i+1}/q_i of successive denominators of the principal convergents p_i/q_i are bounded as before. Furthermore we can conclude as in the proof of Lemma 2 that the partial quotients b_i of $(F_{n-1}+(-1)^{n-1})/(F_{n+1}+(-1)^{n+1})$ are equal to the partial quotients a_i of F_{n-1}/F_{n+1} for $i < n/2-2$. Thus we can conclude as in (3.19) that $|x_1x_2| \gg F_n$ and $|x_1x_3| \gg F_n$ for $0 < |x_1| \ll F_n^{1/2}$.

The most difficult part of the proof is the case where $|x_2|$ is small. Let $F_n/(F_{n+1}+(-1)^{n+1}) = [0;a_1,a_2,\ldots,a_M]$ be the continued fraction expansion and $p_i/q_i = [0;a_1,a_2,\ldots,a_i]$ $(i \leq M)$ the principal convergents of $F_n/(F_{n+1}+(-1)^{n+1})$. Then $(F_{n+1}+(-1)^{n+1})p_{M-1} - F_nq_{M-1} = (-1)^M$ implies that all integral solutions of $a \cdot x = 0$ can be written as

$$\begin{aligned} x_1 &= m_1(-1)^{n+1}q_{M-1} + m_2(F_{n+1}+(-1)^{n+1}) \\ x_2 &= m_1(-1)^M \\ x_3 &= -m_1((-1)^M + (-1)^{n+1}p_{M-1} - m_2F_n \end{aligned} \tag{3.22}$$

with $m_1, m_2 \in \mathbf{Z}$. Since $q_{M-1}/(F_{n+1}+(-1)^{n+1}) = [0;a_M,a_{M-1},\ldots,a_1]$ (cf. Theorem 4 in Chapter I of [La]) and all partial quotients a_i are bounded by 5 (see (3.13)) we can conclude as above that $|x_1x_2| \gg F_n$ for $0 < |x_2| \ll F_n^{1/2}$. If we know that the partial quotients b_i of $(p_{M-1} \pm 1)/F_n$ are equal to a_{M-i+1} for $i < n/6 - C_1$ for some absolut constant $C_1 \geq 2$ then the proof is finished because $a_{M-i} = 4$ for $1 \leq i < n/6-2$ implies that the denominator Q_{i_0} of $P_{i_0}/Q_{i_0} = [0;a_M,a_{M-1},\ldots,a_{M-i_0+1}]$ with $i_0 = [n/6-C_1]$ satisfies $Q_{i_0} \gg\ll F_n^{1/2}$ (see (3.25)). Since the numerators p_{M-i} of $p_{M-i}/q_{M-i} = [0;a_1,\ldots,a_{M-i}]$ and the denominators Q_{i+1} of $P_{i+1}/Q_{i+1} = [0; a_M, a_{M-1}, \ldots, a_{M-i+1}]$ satisfy the same recursion for $i \geq 0$, namely

$$\begin{aligned} p_{M-i} &= a_{M-i} p_{M-i-1} + p_{M-i-2} \\ Q_{i+1} &= a_{M-i} Q_i + Q_{i-1}, \end{aligned} \tag{3.23}$$

we easily get by induction that

$$(F_n, p_{M-1} \pm 1) = (p_{M-i} \pm (-1)^{i-1} Q_{i-1}, p_{M-i-1} \pm (-1)^i Q_i). \tag{3.24}$$

Now $a_{M-i} = 4$ for $1 \leq i < n/6-2$ implies that $Q_i \gg\ll (2+\sqrt{5})^i$ for $1 \leq i < n/6-2$. On the other hand we have $F_i \gg\ll ((1+\sqrt{5})/2)^i$, where $((1+\sqrt{5})/2)^3 = 2+\sqrt{5}$. Hence

$$Q_{i_0} \gg\ll F_{[n/2]} \gg\ll F_n^{1/2}. \tag{3.25}$$

By similar calculations we get

$$p_{M-i-1} \pm (-1)^i Q_i < p_{M-i} \pm (-1)^{i-1} Q_{i-1} \tag{3.26}$$

for $i < n/6 - C_1$ and some explicitely computable constant $C_1 \geq 2$. So the partial quotients b_i of $(p_{M-1} \pm 1)/F_n$ are equal to a_{M-i+1} for $i < n/6 - C_1$. $\square$

4. The Discrepancy of Linear Functions

Let $C_K(s)$ be the set of continuous functions $g : [0,1] \to \mathbf{R}^K/\mathbf{Z}^K$ with arclength $\int_0^1 |dg(t)| = s$ and set

$$\Delta_K(s) = \inf_{g \in C_K(s)} D(g(t)), \tag{4.1}$$

where $D(g(t))$ is the discrepancy of $g(t)$ defined in (1.6). In [Ta] and [Dr] it is shown without use of linear functions that

$$s^{-\frac{K}{K-1}} \ll \Delta_K(s) \ll s^{-\frac{K}{K-1}} (\log s)^{K-1}, \qquad s \to \infty. \tag{4.2}$$

In [Dr] it is also shown that for $K = 2$ we have

$$\Delta_2(s) \gg\ll s^{-2}, \qquad s \to \infty. \tag{4.3}$$

In fact it is possible to prove

Theorem 4.

$$\Delta_2(s) = \frac{1}{2s^2} \left(1 + O\left(\frac{1}{s}\right)\right), \quad s \to \infty. \tag{4.4}$$

Proof. First we will show that $D(f(t)) = (4|c_1 c_2|)^{-1}$, where c_1, c_2 are coprime non-zero integers and $f(t) = (c_1, c_2)\, t \mod 1$. Subdivide $[0,1)^2$ into $|c_1 c_2|$ rectangles $R_{ij} = \left[\frac{i}{|c_2|}, \frac{i+1}{|c_2|}\right) \times \left[\frac{j}{|c_1|}, \frac{j+1}{|c_1|}\right)$ $(0 \leq i < |c_2|, 0 \leq j < |c_1|)$, let $I = [a_1, b_1] \times [a_2, b_2] \subseteq \mathbf{R}^2/\mathbf{Z}^2$ be any rectangle, and let i_k, j_l $(1 \leq k, l \leq 2)$ be defined by $(a_k, b_l) \in R_{i_k j_l}$. Then

$$\int_0^1 \mathbf{1}_{R_{ij} \cap I}(f(t)) = \lambda_2 (R_{ij} \cap I) \tag{4.5}$$

for all rectangles R_{ij} except $R_{i_k j_l}$ $(1 \le k, l \le 2)$. So

$$\begin{aligned} D(f(t)) &= \max_I \left| \int_0^1 \mathbf{1}_{\left(\bigcup_{1\le k,l\le 2} R_{i_k j_l} \cap I\right)}(f(t)) - \lambda_2\left(\bigcup_{1\le k,l\le 2} R_{i_k j_l} \cap I \right) \right| \\ &= \frac{1}{4}\,\lambda_2(R_{ij}) = \frac{1}{4|c_1 c_2|}. \end{aligned} \tag{4.6}$$

Now functions like $f_N(t) = (N, N+1)\,t \mod 1$ immediatly imply

$$\Delta_2(s) \le \frac{1}{2s^2}\left(1 + O\left(\frac{1}{s}\right)\right), \qquad s \to \infty. \tag{4.7}$$

On the other hand, if $g : [0,1] \to \mathbf{R}^2/\mathbf{Z}^2$ is any continuous function with arclength s then let N be the smallest integer satisfying $\sqrt{2}sN + 1 < N^2 - 1$ and subdivide the arc $g([0,1])$ into $K < \sqrt{2}sN+1$ subarcs $g_k = g([t_k, t_{k+1}])$ of arclengths $s_k < 1/(\sqrt{2}N)$ $(0 \le k < K)$. Set $Q_{ij} = \left[\frac{i}{N}, \frac{i+1}{N}\right) \times \left[\frac{j}{N}, \frac{j+1}{N}\right)$ for $0 \le i, j < N$. Then

$$\int_{[0,1/N)^2} \left(\sum_{0\le k<K} \sum_{0\le i,j<N} \mathbf{1}_{(Q_{ij}+x)}(g_k) \right) dx \le \frac{2K}{N^2} \tag{4.8}$$

would imply that there is some $x_0 \in [0,1/N]^2$ such that the sum of the numbers of squares $Q_{ij} + x_0$ such that $g_k \cap (Q_{ij} + x_0) \ne \emptyset$ $(0 \le k < K)$ is bounded by $2K$. But $g(t_k) \in g_k \cap g_{k+1}$ for $0 \le k \le K-2$ so that the number of squares $Q_{ij} + x_0$ such that $g([0,1]) \cap (Q_{ij} + x_0) \ne \emptyset$ is bounded by $2K - (K-1) = K+1$. Thus $K + 1 < N^2$ implies that there is some square $Q_{i_0 j_0} + x_0 \subseteq \mathbf{R}^2/\mathbf{Z}^2$ with $g([0,1]) \cap (Q_{i_0 j_0} + x_0) = \emptyset$. So

$$\begin{aligned} D(g(t)) &\ge \left| \int_0^1 \mathbf{1}_{(Q_{i_0 j_0}+x_0)}(g(t))\,dt - \lambda_2(Q_{i_0 j_0} + x_0) \right| \\ &= \frac{1}{N^2} \\ &= \frac{1}{2s^2}\left(1 + O\left(\frac{1}{s}\right)\right), \qquad s \to \infty. \end{aligned} \tag{4.9}$$

Therefore we only have to show (4.8). Let $f : [0,1] \to [0,1]^2$ be a continuous function with arclength $s = 1/\sqrt{2}$ and set $Q_1 = [0,1)^2$, $Q_2 = [-1,0) \times [0,1)$, $Q_3 = [-1,0)^2$, and $Q_4 = [0,1) \times [-1,0)$. Then (4.8) is implied by

$$\int_{[0,1]^2} \left(\sum_{i=1}^4 \mathbf{1}_{(Q_i+y)}\left(f([0,1])\right) \right) dy \le 2. \tag{4.10}$$

Let $a = \inf\{\alpha_2 - \alpha_1 \mid f([0,1]) \subseteq [\alpha_1, \alpha_2] \times [0,1]\}$ and $b = \inf\{\beta_2 - \beta_1 \mid f([0,1]) \subseteq [0,1] \times [\beta_1, \beta_2]\}$. Trivially $a^2 + b^2 \le s^2 = 1/2$. With this notation we can calculate

$$\begin{aligned} &\int_{[0,1]^2} \left(\sum_{i=1}^4 \mathbf{1}_{(Q_i+y)}\left(f([0,1])\right) \right) dy \\ &= A + 3ab + 2a(1-b) + 2b(1-a) + (1-a)(1-b) \\ &= A + a + b + 1, \end{aligned} \tag{4.11}$$

where A denotes the area of those $y \in [0,1]^2$ with

$$\sum_{i=1}^{4} \mathbf{1}_{(Q_i+y)}\left(f([0,1])\right) = 4. \tag{4.12}$$

So we only have to show that

$$A + a + b \le 1. \tag{4.13}$$

It is clear that we can restrict to the case where $f(t) = (f_1(t), f_2(t))$, $t \in [0,1]$, is continuously differentiable. Set $a' = \lambda_1\left(\{f_1(t) \,|\, f_1'(t) \ge 0\}\right)$, $a'' = \lambda_1\left(\{f_1(t) \,|\, f_1'(t) \le 0\}\right)$, $b' = \lambda_1\left(\{f_2(t) \,|\, f_2'(t) \ge 0\}\right)$, and $b'' = \lambda_1\left(\{f_2(t) \,|\, f_2'(t) \le 0\}\right)$. W.l.o.g. we can assume that $a' \ge a''$ and that $b' \ge b''$. Then we have $a \le a'$, $b \le b'$, $(a'+a'')^2 + (b'+b'')^2 \le 1/2$, and

$$A \le a''b + b''a. \tag{4.14}$$

But now (4.13) follows from $a' + b' + a''b' + b''a' \le 1$, which can be verified by elementary means. □

For $K = 3$ we can use Theorem 2 to obtain

Theorem 5.

$$\Delta_3(s) \gg\ll s^{-\frac{3}{2}}. \tag{4.15}$$

Proof. We only have to prove the upper bound. In order to do this it sufficies to find proper functions $g_N(t)$ with arclengths s_N satisfying $1 \le s_{N+1}/s_N \le C$ for some absolut constant $C > 0$ and $D(g_N(t)) \ll s_N^{-3/2}$.

Set $g_N(t) = a_N t \mod 1$ with $a_N = (F_{6N+1}, F_{6N+2}, F_{6N+2} + 1)$. By Koksma-Erdös-Turan's inequality for functions we have for any positive integer H

$$\begin{aligned} D(a_N t) &\ll \frac{1}{H} + \sum_{0<||h||\le H} \frac{1}{r(h)} \left| \int_0^1 e^{2\pi i (a_N \cdot h) t}\, dt \right| \\ &= \frac{1}{H} + \sum_{0<||h||\le H, a_N \cdot h = 0} \frac{1}{r(h)}. \end{aligned} \tag{4.16}$$

But it is an easy exercise that (3.2) combined with some simple arguments concerning the solutions h with $\min(|h_1|, |h_2|, |h_3|) \gg F_{6N}^{1/2}$ implies

$$\sum_{a_N \cdot h = 0, h \ne 0} \frac{1}{r(h)} \ll F_{6N}^{-\frac{3}{2}}. \tag{4.17}$$

In order to complete the proof of Theorem 5 note that $s_N = |a_N| \gg\ll F_{6N}$ and so we have $1 \le s_{N+1}/s_N \le C$. □

Remark. The use of Koksma-Erdös-Turan's inequality in (4.16) indicates how to prove the upper bound of $D(at)$ in (1.7). On the other hand Koksma-Hlawka's inequality for functions applied to a function $g : [0,1]^K \to \mathbf{R}$ of bounded variation $V(g)$, namely to $g(x) = h \cdot x$, $(h \ne 0)$ reads as

$$\left| \int_0^1 e^{2\pi i (a \cdot h) t}\, dt \right| \le V(h \cdot x)\, D(at), \tag{4.18}$$

where the variation $V(h \cdot x)$ can be estimated by

$$V(h \cdot x) \ll r(h). \tag{4.19}$$

This proves the lower bound of (1.7).

It should be noted that the method of the proof of Theorem 3 and Koksma-Erdös-Turan's inequality for functions can be used to show the existence of an integral lattice point $a \in \mathbf{Z}^K$ with arbitrarily large components such that

$$D(at) \ll \frac{(\log |a|)^K}{|a|}. \tag{4.20}$$

(Compare with [KN,p 154].) This estimate is far away from the upper bound (4.2). Therefore it might be possible to sharpen Theorem 3. It seems that a proof that the exponent $1/(K-1)$ of Theorem 1 is optimal could be used to find linear functions with small discrepancy and maybe one will be able to sharpen the upper bound (4.2) for $K > 3$ by this method as it has been done in Theorem 5 for $K = 3$.

References

[Dr] M. Drmota, *Irregularities of Continuous Distributions*, Ann. Inst. Fourier **39** (1989), 501–527.

[KN] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley and Sons, New York, 1974.

[La] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, 1966.

[Sch] W.M. Schmidt, *Diophantine Approximation and Diophantine Equations*, Notes on lectures delivered at Columbia University and at the University of Colorado, 1990.

[Sie] C.L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. d. Wiss., Math. Phys. Kl. **1** (1929), 1–41.

[Ta] R.J. Taschner, *The Discrepancy of c-Uniformly Distributed Multidimensional Functions*, J. Math. Anal. Appl. **78** (1980), 400–404.

Michael Drmota
Department of Discrete Mathematics
Technical University of Vienna
Wiedner Hauptstrasse 8–10/118
A-1040 Vienna, AUSTRIA